PATENT
P56955

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

IN-ZOO LEE

Serial No.:	*to be assigned*	Examiner:	*to be assigned*
Filed:	13 February 2004	Art Unit:	*to be assigned*

For: METHOD FOR ENCRYPTING DATA OF AN ACCESS VIRTUAL PRIVATE NETWORK (VPN)

CLAIM OF PRIORITY
UNDER 35 U.S.C. §119

Mail Stop Patent Application
Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application, Korean Priority No. 2003-10823 (filed in Korea on 20 February 2003, and filed in the U.S. Patent and Trademark Office on 13 February 2004), is hereby requested and the right of priority provided in 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application.

Respectfully submitted,

Robert E. Bushnell
Reg. No.: 27,774
Attorney for the Applicant

Suite 300, 1522 "K" Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56955
Date: 13 February 2004
I.D.: REB/kf

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0010823
Application Number

출 원 년 월 일 : 2003년 02월 20일
Date of Application FEB 20, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 09 월 23 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.02.20
【발명의 명칭】	억세스 가상 사설망의 데이터 암호화 방법
【발명의 영문명칭】	Method for encrypting data of access VPN
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	박상수
【대리인코드】	9-1998-000642-5
【포괄위임등록번호】	2000-054081-9
【발명자】	
【성명의 국문표기】	이인주
【성명의 영문표기】	LEE, IN ZOO
【주민등록번호】	720917-1770623
【우편번호】	463-030
【주소】	경기도 성남시 분당구 분당동 168-1
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 박상수 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	1 면 1,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	6 항 301,000 원
【합계】	331,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 억세스 가상사설망(Virtual Private Network:VPN)의 가입자가 자사의 가상 사설망에 접속시 데이터 보안을 위해 데이터 암호화 단계를 거치도록 하는 억세스 가상사설망의 데이터 암호화 방법에 관한 것으로서, 사용자 접속 시도 신호에 따라 Dead단계(S100)에서 UP되어 Establish단계(S200)를 수행하고, S200에서는 상호 인증방법, 최대 수신 바이트수, 데이터 압축유무 등등에 관한 LCP 협상이 이루어지며, LCP 협상 조건에 따라 상호 인증이 필요하고 데이터 암호화가 필요하다고 양단에 협상이되면 먼저 Authenticate단계(S300)를 수행하고, S300에서 PAP/CHAP으로 상호 인증을 수행하여, 인증이 정상적으로 끝나면 데이터 암호화를 수행하는 Encryption 단계(S350)를 수행하도록 하므로써, 사용자 인증과정과 더불어 데이터 암호화 과정이 수행되므로, 데이터가 쉽게 노출되지 않게 되어 보안성있는 통신이 이루어지는 효과가 있다.

【대표도】

도 5

【색인어】

암호화, VPN, IPSec, L2TP, PPP

【명세서】

【발명의 명칭】

억세스 가상 사설망의 데이터 암호화 방법{Method for encrypting data of access VPN}

【도면의 간단한 설명】

도 1은 일반적인 L2TP(Layer 2 Tunneling Protocol)를 이용한 억세스 VPN(Virtual Private Network)의 구성에 관한 블럭도,

도 2는 사용자가 L2TP를 이용해 자사의 사설망에 접속하는 과정을 나타내는 흐름도,

도 3은 일반적인 PPP(Point-to-Point Protocol) 동작에 관한 흐름도,

도 4는 본 발명에 적용되는 PPP 패킷 데이터 형식에 관한 도면,

도 5는 본 발명의 바람직한 실시예에 따라 암호화 단계가 포함된 PPP 동작에 관한 흐름도.

<도면의 주요 부분에 대한 부호 설명>

10 : 사용자 단말기 20 : PSTN망

30 : ISP(서비스 제공사업자) 40 : 인터넷망(IP망)

50 : LNS(사설망)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<10> 본 발명은 억세스 가상사설망(Virtual Private Network:이하 'VPN'라 함)의 가입자가 자사의 가상 사설망에 접속시 데이터 보안을 위해 데이터 암호화 단계를 거치도록 하는 억세스 가상사설망의 데이터 암호화 방법에 관한 것이다.

<11> 오늘날 많은 기업들은 분산된 기업내의 통신을 위하여 통신 사업자의 전송장비를 임대하여 그들 자신의 사설통신망을 구축해왔으나, 기업이 사설통신망을 구축하여 운용하는 일은 단순하면서도 어려운 일이었다. 비용측면에서 볼 때 일반적으로 전송장비를 소유하거나 임대하는 데는 많은 비용이 들고 회선구성도 두 지점간에는 비교적 쉽지만 여러 지점간을 연결하는 경우는 매우 어려운 과정을 필요로 한다. 이와 같이 기업의 사설망 구축은 그 범위에 따라 상당한 비용이 소요되므로 이용자들은 자연히 통신비용에 대해서 관심을 갖게 되었다.

<12> 따라서, 통신사업자는 이러한 기업의 요구에 맞춰 여러 가지 사업용 통신 서비스를 제공하여 왔으며, 특히 "가상사설망"이라고 불리는 서비스 개발을 추진해왔다. 가상사설망 서비스는 가입자 자신이 공중통신망 내에서 소프트웨어적으로 망을 정의하고 변경할 수 있기 때문에 통신망 변경시에 물리적인 재구성이 필요없으며 공중통신망을 이용하여 마치 가입자 고유의 사설통신망을 소유하고 있는 것과 같은 효과를 주는 서비스이다. 사설망이란 기업체나 기타 그룹간이 원활한 통신을 위해서 사용하는 독립적인 통신망으로서 지역적인 조건에 관계없이 동일한 사설망 내에서는 단일번호계획을 가질 수 있으며 보안기능측면이나 신뢰성 측면에서 많은 장점을 가지고 있으나 각각의 기업체에서 해당 망을 직접 관리해야 하는 어려움이 있다. 이러한

어려움을 해결하고 사설망이 같는 모든 기능들을 공중통신망을 통해서 제공해주는 서비스가 VPN 서비스이다.

<13> 이러한 VPN 서비스는 공중망을 근간으로 하여 여러 곳에 분산 위치해 있는 기업 등의 여러 수요자들이 그들의 통신 요구량을 마치 자신의 LAN을 통해 통신하는 것과 같은 효과를 가질 수 있으며, 그 계약관계에 의해서 자신의 사설망의 확장이나 구조 재설정 등이 매우 용이하다는 장점을 가진다. 이는 그들이 사용하는 실제 물리적인 망은 공중망이어서 가능한 것으로 그 물리적인 망에 대한 관리는 모두 공중망 운용자가 맡고 있다.

<14> 따라서, 기업간의 인트라넷, 엑스트라넷 등의 구축 시에 공중망을 사용하여 네트워크 구축비용을 줄일 수 있으며, 기업 정보를 보호할 수 있는 VPN의 대두는 불가피한 것으로 보인다.

<15> 그리고, VPN은 인터넷이나 네트워크 서비스 사업자의 공중망을 자사의 WAN 백본처럼 사용하는 네트워크라고 할 수 있다. 이러한 개념은 지난 수년간 인터넷의 급격한 성장에 따른 결과라고 해도 지나치지 않는데, 인터넷을 이용하여 기업의 마케팅 및 영업활동에 최소의 비용으로 최대의 효과를 낼 수 있는 기반이 되고 있다.

<16> 또한 ISP(Internet service provider)들도 이러한 인터넷의 환경변화에 맞춰 꾸준히 백본 용량을 증가시켜 왔고, IP 프로토콜에 대한 지속적인 연구는 기존의 전화망에서나 가능했던 음성, 팩스, 리모트 액세스, LAN-to-LAN 서비스 및 전자상거래에 이르기까지 다양한 서비스를 제공할 수 있는 수준에 도달하고 있는 실정이다. 그러나, 이러한 새로운 인터넷 기반의 서비스들은 QoS(Quality of Service)와 보안이라는 중요한 기술적 문제를 내포하고 있다.

<17> 따라서, 최근에는 충분한 대역폭 확보와 기업내 정보보호를 목적으로 VPN 서비스가 급속히 보급되고 있는 실정이다.

<18> 이러한 기업들이 VPN 도입을 하려고 하는 이유는 다음과 같다.

<19> 정보 공유의 확산, 신속한 의사결정, 사외 네트워크 구성의 필요성 대두, 업무범위의 확대, 이동/재택 근무자의 증가와 같은 업무 환경이 변화하였기 때문이다.

<20> 이하, 현재의 VPN 기술을 여러 가지 형태에 따라 분류하여 설명하기로 한다.

<21> 먼저 망의 형태에 따라 분류하면 다음과 같다.

<22> - Access VPN : 본사와 원격지의 인가된 사용자간의 네트워크

<23> Client-to-LAN 방식을 사용

<24> - Intranet VPN : 본사와 지사간의 네트워크

<25> LAN-to-LAN 방식을 사용

<26> - Extranet VPN : 본사와 사업파트너 또는 고객 등과의 네트워크

<27> 보안정책이 다른 네트워크들을 상호연결, 보안 취약

<28> 그리고, VPN 기술을 연결방식에 따라 분류하면 다음과 같다.

<29> - Client-to-LAN : 기업과 원격지 또는 이동 근무자간 접속

<30> 모뎀, ISDN, xDSL 등 다양한 접속 장비 사용

<31> 원격 사용자의 로컬 POP에 전화 접속후 VPN 기능 이용

<32> - LAN-to-LAN : 다양한 형태의 VPN 장비 존재

<33> 호스트 컴퓨터에 VPN 모듈 탑재

<34> 원격지 VPN 지원

<35> 이중 본 발명에서 사용되는 억세스 VPN은 주로 이동중인 사용자가 모뎀이나 xDSL을 통해 L2TP(Layer 2 Tunneling Protocol), PPTP(Point to point Tunneling Protocol) 등의 PPP 터널링 프로토콜을 이용하여 자사의 사설망에 접속하는 Client-to-LAN 방식 VPN을 말한다.

<36> L2TP는 PPTP와 L2F를 통합한 프로토콜로서, IFTF RFC2661에 정의되어 있다. L2TP의 특징은 2계층의 터널링 프로토콜로 PPP 패킷을 직접 캡슐화하며, 하나의 터널안에 PPP 패킷 종류별 여러 세션 설정이 가능하다.

<37> 이하, L2TP를 예를 들어 억세스 VPN의 구성을 살펴보기로 한다.

<38> 도 1은 일반적인 L2TP(Layer 2 Tunneling Protocol)를 이용한 억세스 VPN(Virtual Private Network)의 구성에 관한 블럭도이고, 도 2는 사용자가 L2TP를 이용해 자사의 사설망에 접속하는 과정을 나타내는 흐름도이다.

<39> 도 1 및 도 2를 참조하면, 억세스 VPN 가입자가 사용자 단말기(10)를 이용하여 자사의 사설망(LNS: L2TP Network Server)에 접속하기 위해, PSTN(Public Switched Telephone Network)망(20)을 통해 ISP(30)에 PPP 접속을 한다(T1). ISP(30)와 접속이 이루어지면 독립적인 2개의 호스트간(peer-to-peer)의 사용자 인증방식인 CHAP/PAP(Challenge Handshake Authentication Protocol/Password Authentication Protocol)를 이용한 사용자 인증과정을 거치게 된다(T2).

<40> ISP(30)는 사용자 인증과정이 성공적으로 수행되면, 사용자와 사설망을 연결해주기 위해 L2TP 터널을 형성한다(T3).

<41> L2TP 터널이 형성되면, 사용자 단말기(10)와 LNS(50)간에 다시 한번 인증과정을 수행한 후(T4), PPP NCP(Network Control Protocol) 협상을 시작한다(T5).

<42> 정상적으로 NCP 협상이 이루어지면, 사용자 단말기(10)와 LNS(50)간에 PPP 세션이 형성되어(T6), 데이터 송수신이 이루어지게 된다(T7).

<43> 상기 과정은 크게, 사용자 단말기(10)와 ISP(30)간에 링크 관련 파라미터를 교환하는 LCP(Link Control Protocol)단계(T1)와, 사용자 인증 단계(T2, T4)와, 사용자 단말기(10)와 LNS(50)간에 상위 프로토콜 관련 파라미터를 교환하는 NCP 단계(T5,T6)로 구분되어 진다.

<44> 이하, 상기 과정을 PPP 동작과 관련지어 설명하기로 한다.

<45> 도 3은 일반적인 PPP(Point-to-Point Protocol) 동작에 관한 흐름도이다.

<46> 사용자 접속 시도 신호에 따라 Dead단계(S10)에서 UP되어 Establish단계(S20)를 수행하게 된다. S20에서는 상호 인증방법, 최대 수신 바이트수, 데이터 압축유무 등등에 관한 LCP 협상이 이루어지며, LCP 협상 조건에 따라 상호 인증이 선택된 경우 Authenticate단계(S30)를 수행한다. S30에서 인증이 실패하면, 접속이 취소되어 Terminate 단계(S50)를 수행하게 된다.

<47> S30에서 인증이 성공적으로 이루어지거나, LCP 협상 조건에서 상호인증을 선택하지 않은 경우, Network 단계(S40)를 수행하여 레이어 3 통신을 위한 정보(IP 주소 할당, DNS서버 주소 할당 등)를 협상한 후, 상호 데이터를 송수신한다.

<48> 이와같이, 억세스 VPN에 사용되는 프로토콜들의 경우 PPP를 이용한 사용자 인증방법만 제공할 뿐 사용자 데이터를 보장하기 위한 별도의 방법이 제공되지 않고 있는 반면, LAN-to-LAN방식의 VPN 구성에 사용되는 프로토콜인 IPSec(Internet Protocol Security protocol)의 경우 ,여러 가지 해쉬 함수와 암호화 알고리즘을 제공하여 안전한 정보 교환을 보장해 주고 있다.

<49> 따라서 억세스 VPN에서 사용되고 있는 PPP 표준 동작 알고리즘에 데이터 암호화를 별도의 조치가 절실히 요청된다.

【발명이 이루고자 하는 기술적 과제】

<50> 따라서 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 억세스 VPN 방식에서 사용되는 레이어 2 터널링 프로토콜에 의해 캡슐화되어 전달되는 PPP 표준 동작 알고리즘의 LCP 협상 조건에 데이터 암호화 과정 수행 여부 항목을 추가하므로써, 억세스 VPN 가입자가 데이터를 안전하게 송수신할 수 있도록 하는 방법을 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<51> 이러한 목적을 달성하기 위한 본 발명에 따른 억세스 가상 사설망의 데이터 암호화 방법은. 인증방법, 데이터 압축여부, 받을 수 있는 최대 데이터 크기, 링크 상태 모니터링, 데이터 암호화 수행여부에 관한 링크 컨트롤 프로토콜(LCP:Link Control Protocol) 협상이 이루어지는 제 1단계; 제 1단계의 LCP 협상 조건에 따라 상호 인증이 필요하다고 양단에 협상이 이루어진 경우, 사용자 아이디(ID)와 패스워드(password)를 체크하는 제 2단계; 제 1 단계의 LCP 협상 조건에 따라 데이터 암호화를 수행하는 것으로 양단에 협상이 이루어진 경우, 데이터 암호화를 수행하는 제 3단계; 제 1단계의 LCP 협상 조건에 따라 사용자 인증 및 데이터 암호화를 수행하지 않는 것으로 양단에 협상이 이루어지거나, 데이터 암호화가 수행된 후, 사용자와 사설망간의 접속을 위해 레이어 3 통신을 위한 정보(IP 주소 할당, DNS서버 주소 할당 등)을 협상하는 NCP(Network Control Protocol) 협상이 이루어지는 제 4단계: 및 사용자와 사설망간에

NCP 협상이 수행되면, 사용자와 사설망간에 세션이 형성되어 데이터를 송수신하는 제 5단계로 이루어지는 것을 특징으로 한다.

<52> 상기 제 1단계의 LCP 협상시, 데이터 암호화 수행여부를 포함하여 협상이 이루어지도록 하기 위해 미리 사용자와 사설망의 LCP 협상 옵션 테이블 상에 데이터 암호화(encryption) 수행 여부를 선택할 수 있는 항목을 추가하여 이루어지는 특징이 있다.

<53> 이하, 본 발명이 속하는 분야에 통상의 지식을 지닌자가 본 발명을 용이하게 실시할 수 있도록 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 상세히 설명한다.

<54> 본 발명에 따른 L2TP(Layer 2 Tunneling Protocol)를 이용한 억세스 VPN(Virtual Private Network)의 물리적인 망구성은 종래와 동일하므로 그 설명은 생략하기로 한다.

<55> 단, PPP 표준 동작 알고리즘의 LCP 협상조건에서 데이터 암호화를 선택할 수 있도록 하는 항목이 추가된 PPP LCP 협상 옵션 테이블을 아래 표 2에 제시한다.

<56> 우선, 기존에 정의된 PPP LCP 협상 옵션 테이블은 표 1과 같다.

<57> 【표 1】

코드	정의
0	Reserved
1	Maximum-Receive-Unit
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression

<58>

【표 2】

코드	정의	비고
0	Reserved	
1	Maximum-Receive-Unit	
3	Authentication-Protocol	
4	Quality-Protocol	
5	Magic-Number	
7	Protocol-Field-Compression	
8	Address-and-Control-Field-Compression	
9	Encryption	새로 추가된 항목

<59> 표 2와 같이 데이터 암호화 과정 유무에 대한 옵션 항목이 추가됨에 따라 LCP 협상 단계에서 데이터 암호화를 수행하는 것으로 협상이 이루어지면, 사용자 인증과정과 함께 데이터 암호화를 수행하는 과정이 추가되어 PPP 동작이 이루어지게 된다.

<60> 이때 옵션들은 한꺼번에 여러 개 보내질 수 있으며 보내지지 않는 옵션 들의 경우 디폴트값을 사용한다.

<61> 도 4는 본 발명에 적용되는 PPP 패킷 데이터 형식에 관한 도면이다.

<62> 도 4를 참조하여 PPP 패킷의 각 필드를 살펴보면, Configure-Request Packet(코드=1)에 여러 LCP 협상 옵션들이 포함되어 각 피어(peer)들에게 전달되는데, 이 옵션들은 'type', 'Length', 'Data' 필드로 구분된다.

<63> 이하, 상기의 옵션 필드 구조를 반영한 본 발명의 바람직한 실시예에 따른 암호화 단계가 포함된 PPP 동작을 살펴보기로 한다.

<64> 도 5는 본 발명의 바람직한 실시예에 따른 암호화 단계가 포함된 PPP 동작에 관한 흐름도이다.

<65> 도 5를 참조하면, 사용자 접속 시도 신호에 따라 Dead단계(S100)에서 UP되어 Establish 단계(S200)를 수행하게 된다. S200에서는 상호 인증방법, 최대 수신 바이트수, 데이터 압축유

무 등등에 관한 LCP 협상이 이루어지며, LCP 협상 조건에 따라 상호 인증이 필요하고 데이터 암호화가 필요하다고 양단에 협상이되면 먼저 Authenticate단계(S300)를 수행한다. S300에서 PAP/CHAP으로 상호 인증을 수행하여, 인증이 정상적으로 끝나면 데이터 암호화를 수행하는 Encryption 단계(S350)를 수행한다.

<66> Encryption 단계(S350)는 운영자의 정책에 따라 가장 적합한 암호화 프로토콜을 선정하여 사용하게 되는데, 일반적으로 많이 사용하고 있는 DES(data encryption standard)를 사용하는 것이 바람직하다.

<67> 이하, 이해를 돕기 위해 DES에 관하여 설명하기로 한다.

<68> DES의 기본원리는 아래 수학식 1과 같다.

<69> 【수학식 1】 text(원문)+Key(패스워드)+encryption 알고리즘= 암호화된 원문

<70> 이때 암호화를 위한 킷(key)값은 사용자 패스워드를 이용한다.

<71> 여기서 encryption 알고리즘은 우선 암호화시킬 메시지를 64비트 블록으로 쪼개고, key는 56비트를 고정크기로 한다. 원문에서 나뉘어진 64비트의 블록은 킷값과 함께 재배치하고, 한 비트의 그룹을 다른 비트 그룹과 대체시키는 등의 과정을 거쳐 알아볼 수 없는 데이터로 믹싱(mixing)한다.

<72> 따라서, 상기 방법에 의해 사용자 단말기(10)로부터 사설망(50)간에 오고가는 데이터는 암호화가 된 상태로 송수신되기 때문에, 외부에 노출될 위험이 없어지게 된다.

<73> 이때 암호화 목적상 사용자 인증은 필수항목이므로 데이터 암호화를 선택하는 경우 사용자 인증 과정은 필수적으로 수행하도록 한다.

<74> 물론, 망의 특성에 따라 사용자 인증 과정이 불필요하다고 판단되는 경우엔 사용자 인증 과정을 선택하지 않아도 될 것이다.

<75> S350단계를 수행하면, 데이터 암호화가 처리된 상태에서 Network 단계(S400)를 수행하여 레이어 3 통신을 위한 정보(IP 주소 할당, DNS서버 주소 할당 등)을 협상한 후, 상호 데이터를 송수신한다.

<76> 여기서, 상호 인증시 PAP의 경우, two-way handshaking 방식으로서 인증을 요청하는 호스트에서 사용자 아이디(ID) 및 사용자 패스워드를 일반 텍스트 형태로 전달하므로 인증정보의 외부 노출이 손쉽게 이루어지고 있다. 따라서 암호화가 필요한 경우 three-way handshaking 방식의 CHAP를 수행하여 사용자 암호가 노출되지 않도록 한다.

<77> CHAP 방식은 인증서버에서 호스트로 챌린지 신호를 보내면, 호스트는 보안을 위해 해쉬 함수를 사용하여 계산한 값을 보내고, 인증서버는 이 값이 일치하면 인증을 해주는 방식이기 때문에 보안이 유지되는 것이다.

<78> 이상 본 발명의 바람직한 실시예에 대해 상세히 기술되었지만, 본 발명이 속하는 기술분야에 있어서 통상의 지식을 가진 사람이라면, 첨부된 청구 범위에 정의된 본 발명의 정신 및 범위를 벗어나지 않으면서 본 발명을 여러 가지로 변형 또는 변경하여 실시할 수 있음을 알 수 있을 것이다. 따라서 본 발명의 앞으로의 실시예들의 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

【발명의 효과】

<79> 이상 설명한 바와 같이, 본 발명에 따르면 PPP 터널링 프로토콜(L2TP, PPTP 등)을 이용하여 사용자가 자사의 사설망에 접속할 때 인터넷이라는 보안성을 지원하지 않는 망을 경유하게 되는데, 이때 LCP 협상 옵션 항목에 데이어 암호화 수행여부 항목을 추가시키므로써 PPP 표준 동작 알고리즘에 사용자 인증과정과 더불어 데이터 암호화 과정을 수행할 수 있도록 하여, 데이터가 쉽게 노출되지 않게 되어 보안성있는 통신을 할 수 있도록 해준다.

【특허청구범위】

【청구항 1】

인증방법, 데이터 압축여부, 받을 수 있는 최대 데이터 크기, 링크 상태 모니터링, 데이터 암호화 수행여부에 관한 링크 컨트롤 프로토콜(LCP:Link Control Protocol) 협상이 이루어지는 제 1단계;

제 1단계의 LCP 협상 조건에 따라 상호 인증이 필요하다고 양단에 협상이 이루어진 경우, 사용자 아이디(ID)와 패스워드(password)를 체크하는 제 2단계;

제 1 단계의 LCP 협상 조건에 따라 데이터 암호화를 수행하는 것으로 양단에 협상이 이루어진 경우, 데이터 암호화를 수행하는 제 3단계;

제 1단계의 LCP 협상 조건에 따라 사용자 인증 및 데이터 암호화를 수행하지 않는 것으로 양단에 협상이 이루어지거나, 데이터 암호화가 수행된 후, 사용자와 사설망간의 접속을 위해 레이어 3 통신을 위한 정보(IP 주소 할당, DNS서버 주소 할당 등)을 협상하는 NCP(Network Control Protocol) 협상이 이루어지는 제 4단계: 및

사용자와 사설망간에 NCP 협상이 수행되면, 사용자와 사설망간에 세션이 형성되어 데이터를 송수신하는 제 5단계로 이루어지는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【청구항 2】

제 1항에 있어서, 상기 제 1단계에서 이루어지는 LCP 협상시,

데이터 암호화 수행여부를 포함하여 협상이 이루어지도록 하기 위해 미리 사용자와 사설망의 LCP 협상 옵션 테이블 상에 데이터 암호화(encryption) 수행 여부를 선택할 수 있는 항목을 추가하는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【청구항 3】

제 1항에 있어서, 상기 제 2단계는,

사용자 아이디 및 패스워드를 텍스트 형태로 전달하는 방식으로 사용자 인증을 제공하는 PAP(Password Authentication Protocol)를 이용하는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【청구항 4】

제 1항에 있어서, 상기 제 2단계는,

해쉬함수를 이용하여 사용자 인증을 제공하는 CHAP(Challenge Handshake Authentication Protocol)를 이용하는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【청구항 5】

제 1항에 있어서, 상기 제 3단계에서 이루어지는 데이터 암호화 방법으로,

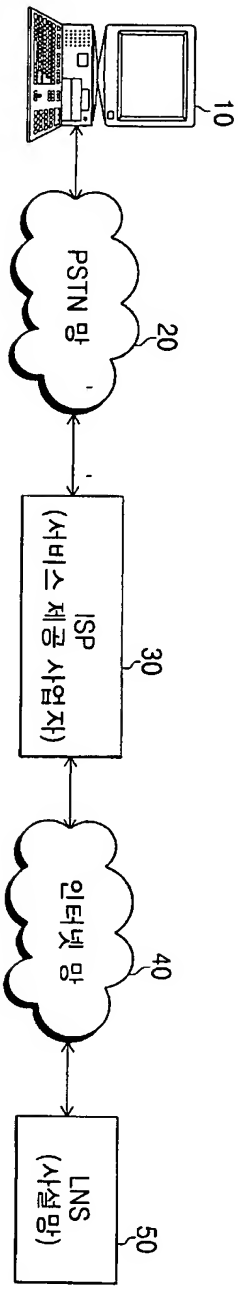
DES(Data Encryption Standard)를 이용하는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【청구항 6】

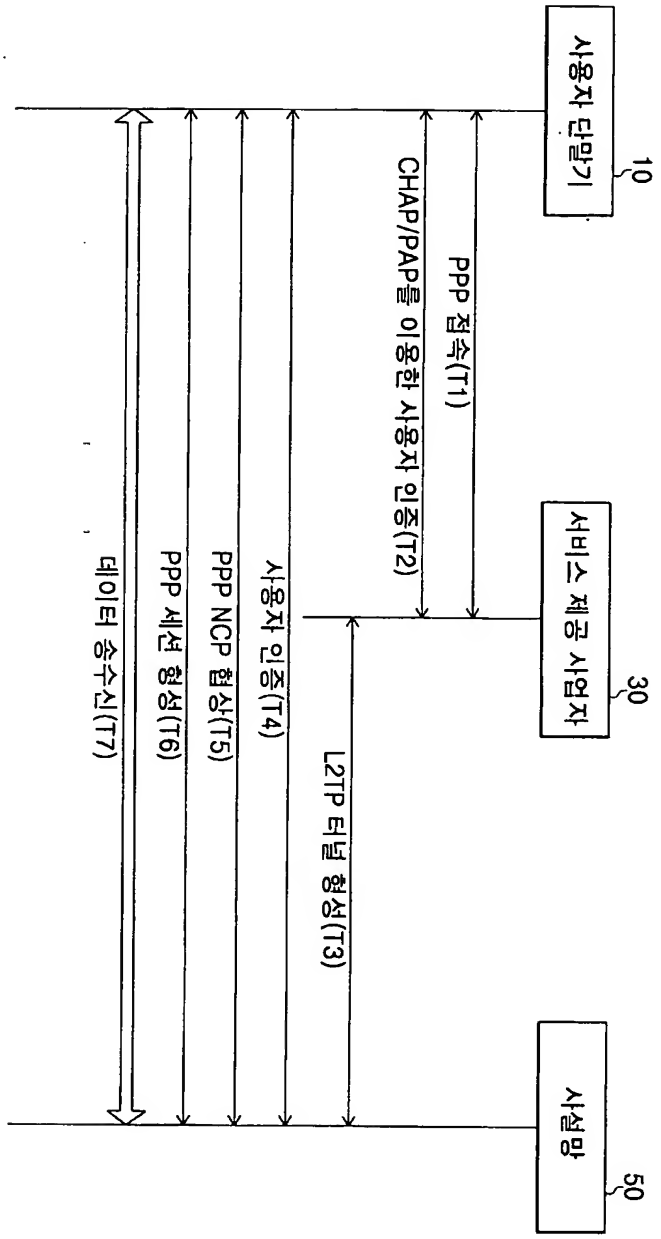
제 1항 또는 제 5항에 있어서, 상기 제 3단계에서 이루어지는 데이터 암호화 수행시, 암호화를 위한 킷(key)값은 사용자 패스워드를 이용하는 것을 특징으로 하는 억세스 가상 사설망의 데이터 암호화 방법.

【도면】

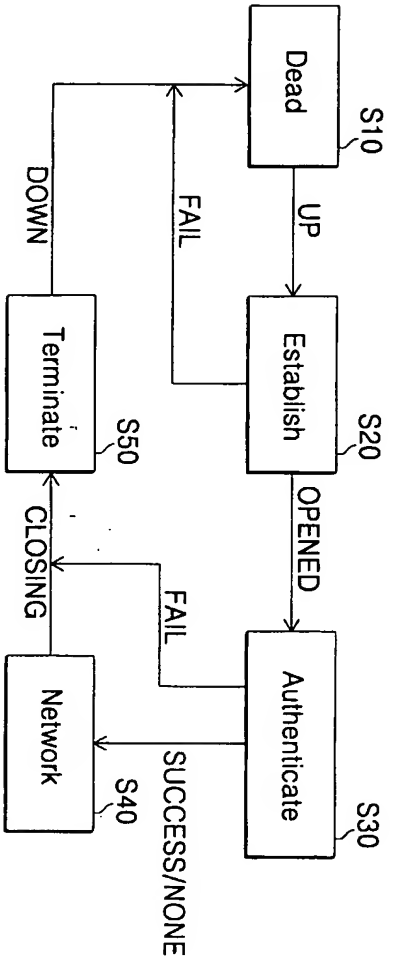
【도 1】



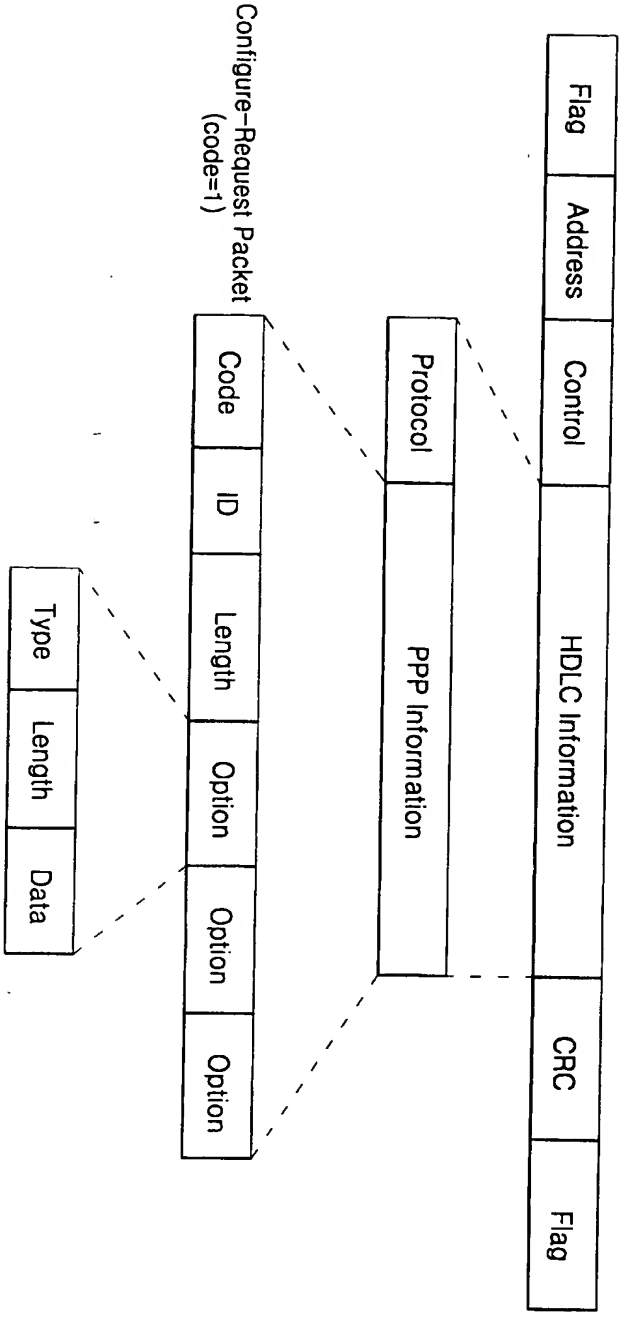
【도 2】


사용자 단말기
10
서비스 제공 사업자
30
사설망
50
PPP 접속(T1)
CHAP/PAP를 이용한 사용자 인증(T2)
L2TP 터널 형성(T3)
사용자 인증(T4)
PPP NCP 협상(T5)
PPP 세션 형성(T6)
데이터 송수신(T7)

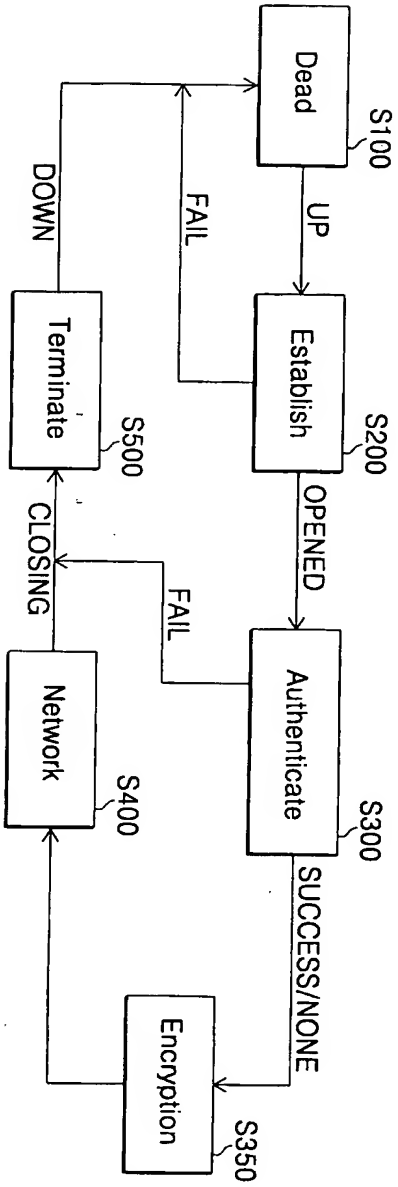
【도 3】


Dead
S10
UP
FAIL
DOWN
Establish
S20
Terminate
S50
OPENED
CLOSING
FAIL
Authenticate
S30
Network
S40
SUCCESS/NONE

【도 4】


Flag
Address
Control
HDLC Information
CRC
Flag
Protocol
PPP Information
Configure-Request Packet
(code=1)
Code
ID
Length
Option
Option
Option
Type
Length
Data

【도 5】


Dead
S100
UP
FAIL
DOWN
Establish
S200
Terminate
S500
OPENED
CLOSING
FAIL
Authenticate
S300
Network
S400
SUCCESS/NONE
Encryption
S350